GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS

Re: Comments on UK Electronic Communications (Security Measures) Regulations 2021

Dear Under Secretary Warman,

We write to you in connection with the draft UK Electronic Communications (Security Measures) Regulations 2021 ("the Security Measures"). We strongly support the underlying objectives of improving cybersecurity outlined in the Security Measures. At the same time, we are concerned with the Security Measures' data localization elements, which we believe will undermine the cybersecurity objectives that these measures are intended to serve. Global Data Alliance (GDA)[1] member companies are highly interested in the Security Measures, as many are active in providing network infrastructure, electronic communications, cloud computing and cybersecurity services inside and outside the United Kingdom. Other GDA members actively utilize such infrastructure and services inside and outside the United Kingdom.

The Security Measures would, in relevant part, require network providers to, among other things:

(1) "maintain the operation of… a public electronic communications network located in the United Kingdom, without reliance on persons, equipment or stored data located outside the United Kingdom." (Art. 3.3(f));
(2) "ensure that tools enabling monitoring or audit cannot be accessed from outside the United Kingdom…" (Art. 4.3(f)); and
(3) "avoid dependence on persons, equipment or stored data located outside the United Kingdom" (Art. 5.3(h)).

To the extent that the above-referenced provisions are intended to achieve cybersecurity objectives, we respectfully suggest that the restrictions do not advance those objectives. As explained in our paper (Cross-Border Data Transfers & Data Localization (globaldataalliance.org), these objectives can be most effectively protected by the adoption of best-in-class security protections that focus on how data is protected, rather than where data is stored or processed.[2]

The above-referenced provisions would require the localization of technologies, data processing and storage, as well as onerous restrictions on the cross-border transfer of data. These aspects of the Security Measures are antithetical to the Measures' stated aim of achieving cybersecurity objectives. Such localization requirements and transfer restrictions often result in *weaker*, not *stronger*, cybersecurity. Cross-border data transfers help improve cybersecurity because these transfers allow for cybersecurity tools to monitor traffic patterns, identify anomalies, and divert potential threats in ways that depend on global access to real-time data. Stronger cybersecurity is enabled by cross-border data analytics and an assertive cyber-defense posture coordinated across IT networks and national boundaries.[3] When governments mandate localization or restrict the ability to transfer and analyze data in real-time, they create unintended vulnerabilities.[4]

The above-referenced provisions of the Security Measures are also antithetical to other policy objectives that are beneficial to the United Kingdom. Cross-border data transfers support international investment, commercial transactions, fraud monitoring and prevention, anti-money laundering, anti-corruption, criminal investigations and enforcement actions, and a broad range of other activities relating to the protection of health, privacy, and security of persons and businesses in the United Kingdom. Jobs and exports are particularly dependent upon data transfers in the advanced industries where the United Kingdom is globally competitive, including in software, finance and other services; advanced manufacturing; and knowledge-intensive industries including biotechnology and medical devices.

The aforementioned aspects of the Security Measures could have the unintended effect of unnecessarily isolating the United Kingdom from its European and North American allies, as well as those farther afield.

The United Kingdom is deeply integrated – both politically and economically – with its European, North American and other allies, and the unprecedented requirement to localize infrastructure, technology and services would be highly disruptive. Significant economic and security impacts could result from efforts to prevent infrastructure and service providers from deploying best-in-class equipment, technology and services from trusted partner countries to support the United Kingdom's security, commercial and other needs. Why would the United Kingdom willingly cut itself off from that access, not to mention from the commercial benefits of digital connectivity with its allies around the world?

Conclusion

The ability to transfer data between the United Kingdom and its neighboring and allied countries is critical to the achievement and preservation of a secure, free and prosperous international political and economic environment. Unnecessary data localization requirements and data transfer restrictions impair the ability of UK and enterprises from trusted partner countries to support infrastructure security, provide cybersecurity services, and (more broadly) engage in international trade, investment, or commercial transactions in the United Kingdom. From this perspective, the aforementioned aspects of the Security Measures warrant careful review. As the Bill goes through the parliamentary process and technical measures are being drafted, we also urge the UK Government to ensure stakeholders' formal feedback is taken on-board. We thank you for the opportunity to share these views. Please do not hesitate to contact us with any questions.

Sincerely yours,

Isabelle Roccia
Global Data Alliance

---

[1] The Global Data Alliance is a cross-industry coalition of companies that are committed to high standards of data responsibility and that rely on the ability to transfer data around the world to innovate and create jobs. GDA members include BSA members and Abbott, American Express, Amgen, AT&T, Citi, Cortex, ExxonMobil, General Motors, Lumen, LEGO, Mastercard, Medtronic, Panasonic, Pfizer, RELX, Roche, United Airlines, Verizon, Visa, and UDS Technology. BSA members include Adobe, Atlassian, Autodesk, Bentley Systems, Box, CNC/Mastercam, DocuSign, IBM, Informatica, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Slack, Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday. BSA | The Software Alliance administers the Global Data Alliance. For more information on the Global Data Alliance, please see: https://www.globaldataalliance.org/downloads/aboutgda.pdf

[2] Global Data Alliance, *Cross-Border Data Transfers and Data Localization* (2020), at: https://www.globaldataalliance.org/downloads/02112020GDAcrossborderdata.pdf; *see also* BSA | The Software Alliance, *The BSA Framework for Secure Software* (2020), at: https://www.bsa.org/files/reports/bsa_framework_secure_software_update_2020.pdf

[3] Global Data Alliance, *Cross-Border Data Transfers and Data Localization* (2020), at: https://www.globaldataalliance.org/downloads/02112020GDAcrossborderdata.pdf. For example, cloud services delivered across-borders provide security advantages over alternative IT delivery approaches (on-premises or local cloud services):

- Physical Security: Certified personnel can carefully monitor servers 24/7 to prevent physical breaches, and can apply consistent protocols over a small number of locations.
- Data Security: CSPs can ensure data integrity through use of state-of-the-art encryption protocols for data at-rest and in-transit. CSPs can establish redundant backups of data in geographically dispersed data centers, mitigating risk of loss in the event of power outages or natural or manmade disasters.
- Advanced Threat Detection: CSPs leverage state-of-the-art enhanced security intelligence They use regular penetration testing to simulate real-world attacks and evaluate security protocols against emerging threats.
- Automated Patch Deployment: Automated and centralized patch deployment and realtime updates to network security protocols work to protect systems from newly identified vulnerabilities.
- Incident Management and Response: CSPs maintain global teams of incident response professionals to respond and mitigate the effects of attacks and malicious activity.
- Certification: CSPs are typically certified to international security standards, and go through regular audits to maintain their certifications.

[4] *See id.*